REMARKS/ARGUMENTS

Claims 1-51 stand rejected in the outstanding Official Action. Claims 1, 4, 34 and 37 have been amended and therefore claims 1-51 remain in the application.

The Examiner's acknowledgment of Applicants' claim for priority and receipt of the certified copies of the priority documents is very much appreciated. Additionally, the Examiner's indication of acceptance of the drawings is appreciated. Finally, the Examiner's consideration of the prior art in Applicants' previously submitted Information Disclosure Statement is appreciated.

Independent claims 1 and 34 stand rejected under 35 USC §102 and/or §103 as anticipated/unpatentable over Motorola ("M68040 User's Manual"). In order to support a rejection under §102, the Examiner must establish that all claimed elements and their claimed interrelationships are actually shown in a single reference, whereas under §103 the burden is on the Examiner to show that each of the claimed elements and claimed interrelationships are either shown or would be obvious to one of ordinary skill in the art in view of the single Motorola reference. As will be understood by reviewing the following portions of Applicants' claims and the Motorola reference, there are structures and structural interrelationships which are simply not shown at any point in the Motorola reference.

It is noted that Applicants' independent claims 1 and 34 specify the operation of a processor "in a plurality of modes and a plurality of domains." While the Examiner directs his rejection to "non-secure and secure **modes**" (page 2, section 3, emphasis added), he apparently ignores Applicants' claim language which also recites "a secure **domain** and a non-secure **domain**" (claim 1, line 3, emphasis added). The existence of the secure and non-secure domains

are discussed at length within the description of the present application. Importantly, and not addressed by the Examiner in his rejection, these **domains** provide a mechanism for handling security at the hardware level.

In effect, the non-secure and secure domains establish separate worlds for the processing system. The non-secure world groups all hardware and software accessible to non-secure applications that do not require security, whereas the secure world groups all hardware and software into a domain which is only accessible when executing secure code. This is entirely different from the operating "modes" to which the Examiner refers in his rejection.

As discussed in Applicant's specification and particularly in the Background of the Invention portion beginning at page 1, line 14, there is a discussion of the many instances where data used by one application may be sensitive data that should not be accessible by other applications that can be run on the same processor. One example of the above is that of a "smart card" where the application might be a security application which uses sensitive data, such as a secure key, to perform validation, authentication, decryption and the like. As noted in the specification, it is important to ensure that such sensitive data be kept secure so that it cannot be accessed by other applications – for example, hacking applications that have been loaded, knowingly or unknowingly, onto the data processing apparatus with the purpose of seeking access to that secure data.

The known approach, which is reflected in the Motorola User's Manual, is to use an operating system which provides sufficient security to ensure that the secure data of one application cannot be accessed by other applications running under the control of the operating

system. However, as noted in the specification, as such systems become more complex, it becomes increasingly difficult to ensure proper security within the operating system itself.

Applicants' claim 1 specifies a processor which is operable not only in a plurality of modes (as the Examiner correctly surmises regarding the non-secure mode and the secure mode), but also a plurality of domains (which language the Examiner apparently has ignored - "said plurality of domains comprising a secure domain and a non-secure domain"). Applicants' independent claims have been modified to make clear that multiples of the plurality of modes are replicated in the secure domain and also in the non-secure domain for providing multiple non-secure modes and multiple secure modes as specified in paragraph 1 of claim 1 (similar language is utilized in method claim 34). Applicants have amended independent claims 1 and 34 to clarify this limitation which is supported by the application as originally filed, see for example Figures 3 and 21 and their associated descriptions on pages 22-23 and 43-48 (specifically page 48, lines 9-12).

The error in the rejection is that the Examiner equates the non-secure domain and consequent non-secure mode terminology used in claim 1 with the "user mode" described in the Motorola reference and the secure domain terminology and consequent secure mode used in claim 1 with the "supervisor mode" also disclosed in the Motorola reference. However, while a possibly convenient analogy, the Examiner ignores the restriction in the claim concerning the "plurality of domains." In the Motorola reference, there is only a single domain, i.e., the non-secure domain, and the user mode and the supervisor mode are two different non-secure modes, not two different domains. The current amendment to claim 1 clarifies that there is a significant distinction between modes (which are disclosed in Motorola) and domains (which are not

disclosed in Motorola). Motorola provides no teaching of replicating multiple modes in a secure domain and a non-secure domain, with the replicated modes in the non-secure domain being referred to as non-secure modes and those replicated modes in the secure domain being referred to as secure modes.

Based upon the clarified wording of the first paragraph of claim 1, it is clear that Motorola fails to disclose the subject matter of Applicants' independent claims 1 and 34 and any further rejection thereunder is respectfully traversed.

Applicants would also point out that Applicants' independent claims also recite first and second sets of tables and confirms the interrelationship between the processor and those sets of tables and the manner in which they are accessed by the memory management unit. Applicants have modified the last paragraph of claims 1 and 34 to state that "when said memory access request pertains to said non-secure domain, the predetermined table in said first set of tables comprises a table managed by the processor when operating in one of said non-secure modes, but the predetermined table in said second set of tables preventing access to physical addresses and forming a secure memory." This language is also absent from the Motorola reference.

Instead, the Motorola disclosure indicates that all tables are managed by the supervisor mode and, as discussed above, that supervisor mode is a non-secure mode like the user code and accordingly cannot be equated with the secure domain identified in claim 1 which is explicitly stated as not being a non-secure mode.

In view of the clarification of the first and second sets of tables and their operating interrelationship with respect to the secure and non-secure modes as defined in Applicants' claim, it is clear that this is not disclosed or even envisioned in the Motorola reference. Should

the Examiner be of the opinion that the limitations relating to the secure domain and non-secure domain in the first full paragraph of Applicants' claim 1 or the limitations relating to the first and second sets of tables in the last paragraph of claims 1 and 34 are somewhere present in the Motorola disclosure, he is respectfully requested to identify the specific chapter and page number and the approximate line number of any such disclosure. Absent any disclosure, any further rejection of independent claims 1 and 34 in view of the Motorola reference is respectfully traversed.

Claims 2-6, 22-33, 35-39 and 44-51 stand rejected under 35 USC §103 as unpatentable over Motorola in view of Chauvel (U.S. Publication 2002/0073282). Inasmuch as these claims ultimately depend from independent claims 1 and 34, the above comments distinguishing claims 1 and 34 from the Motorola reference are herein incorporated by reference. The Examiner does not allege that Chauvel teaches the structures and interrelationships of the first and last full paragraphs in Applicants' independent claims (missing from Motorola). Therefore, even if combined, the Motorola/Chauvel combination would not disclose or render obvious the subject matter of independent claims 1 and 34 or claims dependent thereon.

Claims 7-21 and 41-43 stand rejected under 35 USC §103 as being unpatentable over the Motorola/Chauvel combination in further view of Vishin (U.S. Patent 5,860,146). The above comments regarding Motorola by itself and the Motorola/Chauvel combination are herein incorporated by reference. The Examiner does not allege that Vishin teaches the missing structure and structural interrelationship set out in Applicants' independent claims 1 and 34 (first and last paragraphs) (missing from Motorola) and therefore dependent claims 7-21 and 41-43 cannot be obvious in view thereof.

Having responded to all objections and rejections set forth in the outstanding Official Action, it is submitted that, as amended, claims 1-51 are in condition for allowance and notice to that effect is respectfully solicited. In the event the Examiner is of the opinion that a brief telephone or personal interview will facilitate allowance of one or more of the above claims, he is respectfully requested to contact Applicants' undersigned representative.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100